WHAT IS CLAIMED IS:

1. A personal authentication method using biological information,

wherein during registration, acquired biological information is frequency-analyzed using a plurality of frequencies to generate a feature for each frequency and register the feature, and

wherein the method comprises the steps of:

selecting a frequency used for frequency analysis for authentication from the plurality of frequencies;

performing frequency analysis for acquired biological information of a person to be authenticated using the selected frequency to generate a feature for the frequency; and

comparing the generated feature with the feature generated for the same frequency during the registration to perform personal authentication.

2. The method of Claim 1, wherein the biological information is an image of an iris of an eye.

3. The method of Claim 2, wherein the selection of the frequency during the authentication is performed based on a resolution of an iris image taken during the authentication.

4. The method of Claim 3, wherein the resolution of the iris image is determined from the iris image itself.

5. The method of Claim 4, wherein the resolution of the iris image is determined based on the length of a circumference corresponding to the boundary between the iris and the pupil of the iris image.

6. The method of Claim 3, wherein the resolution of the iris image is determined from information on an apparatus with which the iris image was taken.

7. The method of Claim 1, wherein the selection of the frequency during the authentication is performed based on authentication precision for each combination of the plurality of frequencies.

8. The method of Claim 7, wherein the authentication precision is calculated using a distribution of authentication scores between identical persons and a distribution of authentication scores between different persons.

9. The method of Claim 1, wherein the authentication precision during the authentication is estimated from the

selected frequency.

10. The method of Claim 9, wherein the authentication precision is estimated using a distribution of authentication distances between identical persons and a distribution of authentication distances between different persons.

11. The method of Claim 9, wherein whether or not the person to be authenticated should be finally authenticated is judged according to the estimated authentication precision.

12. The method of Claim 9, wherein a right to be bestowed on the person to be authenticated after the authentication is controlled according to the estimated authentication precision.

13. The method of Claim 9, wherein whether or not re-authentication is performed is judged according to the estimated authentication precision.

14. A personal authentication device using biological information,

wherein during registration, acquired biological information is frequency-analyzed using a plurality of frequencies to generate a feature for each frequency and register the feature, and

wherein the device comprises:

means for selecting a frequency used for frequency analysis for authentication from the plurality of frequencies;

means for performing frequency analysis for acquired biological information of a person to be authenticated using the selected frequency to generate a feature for the frequency; and

means for comparing the generated feature with the feature generated for the same frequency during the registration to perform personal authentication.

15. The device of Claim 14, wherein the biological information is an image of an iris of an eye.